AIR WAR COLLEGE

AIR UNIVERSITY

AVOIDING THE NEXT FAILURE OF IMAGINATION:

HIGHLIGHTING OPPORTUNITIES FOR NATIONAL GUARD CYBER CIVIL SUPPORT TEAMS THROUGH AN ANALYSIS OF THE NATIONAL CYBER RESPONSE CAPACITY GAP USING 9/11 COMMISSION REPORT METHODOLOGIES

by

Gent Welsh, Colonel, WA ANG

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Colonel Robert Douglas, USAF

13 February 2014

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the United States government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Colonel Gent Welsh is a United States Air Force Master Cyberspace Operations Officer in the Washington Air National Guard assigned to the Air War College, Air University, Maxwell AFB, AL. He graduated from Eastern Washington University with a Bachelor of Arts degree in English in 1995 and again in 2003 with a Master of Science in Communications.

Colonel Welsh began his career by enlisting in the United States Air Force in 1988 as a Security Policeman. He was commissioned in the Air National Guard in 1994, and has spent nearly all of his career in command assignments at the flight, detachment, squadron, and group level. His most recent assignment was as the Director, J-6, and Chief Information Officer for the Washington National Guard where he worked extensively on domestic cyberspace security matters.

Abstract

The threat of a catastrophic cyber attack occurring within the United States is a topic routinely discussed at the highest levels of our national government. However, despite the threat rhetoric, the reality is that the United States government is simply not doing enough to ensure the necessary response forces are created and available across the nation to directly assist in the domestic response and recovery from a crippling cyber attack.

This research paper outlines the current state of cyber response capability within the nation using a framework contained in the 9/11 Commission Report. Using the Commission's template outlining failures of imagination, capabilities, policy, and management, this paper breaks down these four failures from a catastrophic cyber attack response respective.

In looking at the failure of imagination, this paper explores the gap that exists between the talk of a "cyber 9/11" attack and our actual ability to respond and recover from such a devastating event. The failure of capabilities section outlines current Department of Defense and Department of Homeland Security capabilities and how those capabilities may not be adequate to support domestic state and local response requirements. The policy failure section describes the lack of adequate policy frameworks currently in place to deal with a cyber response. And last, the management failure section discusses the need to view cyber response from a "bottom up" versus "top down" perspective.

This paper concludes with a recommendation for how National Guard Cyber Civil Support Teams could be created, and a recommendation that Congress take steps to immediately address these capability gaps.

Introduction

After the event, of course, a signal is always crystal clear; we can now see what disaster it was signaling since the disaster has occurred. But before the event it is obscure and pregnant with conflicting meanings.

- The 9/11 Commission Report

Talk of a "Cyber 9/11" headlines contemporary media reports concerning our national vulnerability to a significant cyber attack. In early 2012, Senator Lieberman rose to the Senate floor to declare "Mr. President, I know it is February 14, 2012, but I fear that when it comes to protecting America from cyber-attack it is September 10, 2001, and the question is whether we will confront this existential threat before it happens. Would-be enemies probe the weaknesses in our most critical national assets – waiting until the time is right to cripple our economy or attack a city's electric grid with the touch of a key. The system is blinking red. Yet, we fail to connect the dots – again."[1]

According to the *National Security Strategy* of May 2010, "Cybersecurity threats truly represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale."[2]

Despite the ominous warnings of cyber threats, the nation's, and specifically the Department of Defense's (DOD), collective ability to respond and mitigate the conditions resulting from a catastrophic cyber attack within the homeland is questionable. While the

current DOD Strategy for Homeland Defense and Defense Support to Civil Authorities (DSCA) mentions cyber 22 times,[3] a recent report from the Governmental Accountability Office (GAO) criticizes DOD's cyber response preparation. This report states "although DOD has prepared guidance regarding support for civilian agencies in a domestic cyber incident and has an agreement with the Department of Homeland Security (DHS) for preparing for and responding to such incidents, these documents do not clarify all key aspects of how DOD will support a response to a domestic cyber incident."[4] Additionally, the GAO finds "we recommend that DOD update guidance on preparing for and responding to domestic cyber incidents to align with national-level guidance and that such guidance should include a description of DOD's roles and responsibilities."[5]

Recent efforts by the DOD, specifically, U.S. Cyber Command, to create Cyber Mission Forces (CMF) and Cyber Protection Teams (CPT)[6] to fulfill these roles and responsibilities for responding to a domestic incident, however, are even too limited in focus. DOD's current answer to addressing the domestic cyber response concerns raised over the past year has been the creation of 39-person CPTs with the mission of "defense of the DOD Information Network (DODIN) and assistance outside the DOD when required and authorized."[7] However, the mission of these CPTs may not anticipate all the potential requirements relating to DOD and National Guard (NG) elements supporting domestic cyber responses at the state, local, and even private industry levels…the true "ground zero" where significant cyber issues will actually be managed. Left neglected are the multitude of cities, counties, states, and private sector critical infrastructure/key resources (CIKR) that will be clamoring for some type of governmental, most likely DOD and NG, assistance should they experience the devastating results of a cyber attack.

This paper examines the current domestic cyber response capacity gap from the framework of failures contained in Chapter 11 of the 9/11 Commission Report titled "*Foresight – And Hindsight.*" This report highlighted failures of imagination, policy, capabilities, and management[8] that lead up to the 9/11 attacks. This framework provides a useful lens for evaluating the current state of cyber response in the nation. This paper conducts an examination of these failures from a cyber response perspective and concludes with a recommendation for creating NG Cyber Civil Support Teams to immediately raise the level of cyber response capacity across the nation.

Imagination

While there is recognition at the national level concerning the possibility of a significant cyber attack occurring domestically in the future, the true failure of imagination lies within the unaddressed gap that exists between the rhetoric surrounding the nature of the cyber threat and our actual resource capacity to respond and recover from an attack. However, federal efforts thus far have principally emphasized efforts to prevent cyber attacks, rather than anticipate response considerations. Since 2000, federal government strategies have consistently emphasized the importance of information sharing, partnerships, analysis and warning capabilities, and coordinating efforts in cyberspace among relevant entities to minimize the impact of incidents.[9] While these information sharing and coordinating mechanisms are vitally important, they have done little to anticipate and develop actual response capacity that would be needed post-attack. In remarks before Congress in October 2013, Charley English, Director of the Georgia Emergency Management Agency, stated, "while the pre-event aspects of cybersecurity maintain a high level of importance, so too will the post-event considerations."[10]

In early 2013, both houses of Congress introduced legislation to address this capacity gap by specifically tasking the NG to develop "Cyber and Computer Network Incident Response Teams." Introduced as the "*Cyber Warriors Act of 2013*" in *Senate Bill 658* and *House Bill 1640*, these bills aim to address the cyber response capability gap by directing the DOD to "establish in each of the several States and the District of Columbia a separate team of members of the NG to perform duties relating to analysis and protection in support of programs to prepare for and respond to emergencies involving an attack or natural disaster impacting a computer, electronic, or cyber network."[11] In commenting on *Senate Bill 658* which she co-sponsored, Senator Patty Murray of Washington stated, "the *Cyber Warriors Act* is a good first step in capitalizing on the good work NG units are doing everyday across America. But there is certainly more work to be done. We must continue to provide cyber guards the tools and resources necessary to carry out their mission of safeguarding our economy, critical infrastructure, and citizens in this new era of security at home and abroad."[12]

Unfortunately, the introduction of the *Cyber Warriors Act* was not met with any enthusiasm within the DOD. According to minutes from a June 2013 meeting of the NG's Cyber General Officer Advisory Committee, "the Office of the Secretary of Defense (OSD) remains opposed to both bills or any other legislation directed towards the National Guard. OSD concerns stem from the notion that any legislation specific to the NG would take resources and focus away from the Resource Management Decision (RMD) directed CMF activation."[13]

Prospects in Congress for bill passage are equally as dim. Despite hearings on cyber response capacity,[14] the governmental transparency website, govtrack.us, gives the House bill a four percent chance of passage while giving the Senate bill a one percent chance,[15] contributing to the perpetuation of this failure of imagination. Outside of this proposed legislation, there is

little else going on nationally from an imagination perspective to address this gap between threat and response capacity on a broad scale.

Policy

While imagination is the starting point to consider when evaluating cyber response gaps, a brief examination of the current failure of policy provides a greater understanding into why cyber response processes have been difficult to establish.

The *DOD Strategy for Operating in Cyberspace* of July 2011 calls for "paradigm-shifting approaches such as the development of Reserve and NG cyber capabilities that can build greater capacity, expertise, and flexibility across DOD, federal, state, and private sector activities."[16] However, the policy failure in this strategy is the "paradigm shifting" approach has not been displayed yet with respect to building domestic cyber response capabilities within the NG, focused not exclusively on supporting DOD networks, but on supporting domestic state and local cyber response requirements.

DOD's exclusive focus on creating Title 10 (Armed Forces) capacity relative to the NG is clearly evident in a May 2013 letter from Deputy Defense Secretary, Ashton Carter, and Deputy Secretary of Homeland Security, Jane Holl Lute, to Governors Terry Branstad and Martin O'Malley, co-chairs of the Council of Governors. In this letter, DOD and DHS write, "In response to the Governors' interest in examining how the NG can serve as a cyberspace resource to the States as well as optimize NG contributions to DOD's cyber mission, DOD will spearhead efforts to share DOD's emerging cyberspace force structure and cyberspace workforce vision with the States. In a coordinated effort, U.S. Cyber Command, U.S. Northern Command, and the

National Guard Bureau (NGB) are working to build a Reserve component framework which integrates the NG into DOD's Title 10 cyberspace force structure."[17]

While approaches integrating NG forces into Title 10 structures may have merit from a DOD perspective, they do little to alleviate potential domestic "tugs of war" for these same forces when domestic cyber events occur in a state or territory. Left unaddressed are state and territory requirements to rely on these forces for an on-scene response at the actual incident site. Evidence shows current CMF proposals do not put domestic state and local response capacity as a first priority[18] calling into question DOD "paradigm-shifting" policy. This lack of formal response capability commitment may cause local cyber first responders and affected CIKR operators to question the commitment and availability of NG teams who may be subjected to mobilization or re-deployment elsewhere as part of a larger DOD response. The January 2014 report from the National Commission on the Structure of the Air Force also addressed DOD response requirements outside of Title 10 by stating, "without a better mechanism to capture the Governors' needs and other DSCA requirements, the Air Force and DOD risk building a force structure that does not adequately account for the DSCA mission."[19]

However, current DOD policy for DSCA appears to work against the notion of "paradigm-shifting flexibility" for the NG according to the recently published *DOD Instruction 3025.22, Use of the National Guard for DSCA*. This document states, "The use of the NG for DSCA will not be approved to perform DSCA operations or missions at the direct request to DOD of a State or local civil authority, or to perform activities that the Secretary of Defense determines to be a State's responsibility, including activities performed under a mutual aid and assistance agreement."[20]

In further examining the issue of policy failure from a "whole of government" perspective, *Presidential Policy Directive-21* (Critical Infrastructure Security and Resilience) signed in February of 2013 gives DHS the primary role to "coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure;"[21] however, DHS has yet to publish a final version of the *National Cyber Incident Response Plan* (NCIRP),[22] despite its existence in draft form for nearly three years.

In the draft NCIRP, DHS, in referring to State governors, writes, "Chief Executives should be prepared to request additional resources from the Federal Government, including under the Stafford Act, in the event of a cyber incident that exceeds their government's capabilities."[23] Yet, as will be explored in greater detail under the "management" section of this work, the very process for even requesting additional resources is completely absent, adding to this failure of policy.

Capabilities

While understanding current failures of imagination and policy is important for background, a deeper understanding is needed of the true dearth of response capability that is available now to respond to a domestic cyber attack.

In addressing the capabilities failure, Senator Patrick Leahy commented on the *Cyber Warriors Act* by stating that there exists "a shortfall of both capability and capacity at the federal, state, and local levels to prepare, respond, and mitigate the effects of cyber events."[24] The recently published *National Preparedness Report* by the Federal Emergency Management Agency (FEMA) in March of 2013 stated, "cyber efforts have matured over the past year, but work remains in this complex capability, including increasing state cyber capabilities."[25] Also

contained in the FEMA report were the results of the 2012 State Preparedness Report which stated, "78 percent of states and territories confirmed cybersecurity as a high-priority capability to have," but ranked cyber as the lowest rated actual capability possessed out of 31 assessed areas.[26]

Presidential Policy Directive-21, signed in March of 2013, assigned DHS the responsibility to "provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure."[27] However, DHS lacks a comprehensive domestic cyber response capability as well, and would likely turn to DOD to provide response assistance according to a memorandum signed in 2010 between DOD and DHS.[28] In a catastrophic cyber attack, the federal response capacity found in DHS organizations such as the United States Computer Emergency Response Team (US-CERT) and the Industrial Control System Computer Emergency Response Team (ICS-CERT) would be considered, in military terms, a "high-demand, low-density" asset and would likely be saturated quickly with mission assignments and unavailable for a state or local response.

Since the US has not yet fallen victim to a crippling cyber attack, we can only look to ICS-CERT's current capacity to conduct assessments of CIKR across the country as an indicator of their limited capability. According to the DHS *ICS Year in Review, 2012,* between fiscal years 2010 and 2012, ICS-CERT provided on-site assessments of 31 energy companies,[29] amounting to roughly 10 visits a year across the nation. However, there are over 200 energy utility companies in the US.[30] Even if DHS had the resources to visit each one of the electrical utilities in the US in a preventative, pre-attack assessment mode, every energy utility could expect a DHS visit once every 20 years if DHS kept to its current schedule. More troubling in

this same report, DHS assessed elements of only 11 of the 18 overall total CIKR sectors in FY10, 14 of the 18 in FY11, and 15 of the 18 in FY.[31] Despite dedicating an entire publication[32] to securing the Dams CIKR sector, DHS has been able to only assess one dam in FY10 and none in FYs 11 and 12.[33] Yet according to Army Corps of Engineers figures, there are over 27,000 dams with potential cyber control systems risks operated by federal, state, local, and utilities across the country.[34]

Turning to current DOD cyber response capabilities, the *DOD Strategy for Cyberspace* outlines five key strategic initiatives including "Initiative #3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy."[35] However, this research has not found a single DOD cyber unit identified with the primary mission to partner with and assist officials and entities at the domestic (state and local) level to manage cyber attack consequences. The challenge of creating domestic cyber response capability should not be this difficult. For the DOD, creating domestic-only force structure in the NG is nothing new. Over the past 15 years, DOD, with help from Congress, has created domestic-only capabilities within the NG such as Weapons of Mass Destruction (WMD) - Civil Support Teams (CST); Chemical, Biological, Radiological, Nuclear and High Yield Explosive (CBRNE) enhanced response force packages (CERF-P); and Homeland Response Forces (HRF),[36] yet not a single dedicated domestic response capability in cyber exists today.

Lack of dedicated DOD domestic cyber capability notwithstanding, the NG is in a unique position to respond to cyber events across the US by leveraging existing emergency management relationships already well-established in each state and territory. For the past decade, the NG, through the Departments of the Army and Air Force, has been steadily investing in federally-

traced cyber missions. Currently, the Air National Guard has nine existing cyber units in numbered squadrons across the US,[37] while the Army National Guard has Computer Network Defense Teams in 53 of 54 states and territories.[38] However, this research has revealed none of these units have domestic cyber response in their federal mission description, leaving their ability to respond locally in a federal status with clear authorities given the DSCA constraints, debatable. The reality is, current NG cyber missions only have a clear trace to federal requirements, centered mostly on DODIN protection. The primacy of this federal mission focus leaves nothing clearly identified for the NG to support a domestic cyber response, contributing to a failure of capabilities, and a failure of DOD's "paradigm-shifting" approach.

Management

Finally, an examination of existing management shortfalls concerning our cyber response ability provides a basic framework for understanding that "all responses are local." Both a local capability as discussed above, and a well-understood management process are needed for an effective cyber response.

In further examining the concept that "all responses are local," the *National Response Framework* (NRF) is the key document outlining how disaster responses are managed, from the local incident site up to the federal level. According to the NRF, "most incidents begin and end locally and are managed at the local level."[39] The NRF further states, "scalable, flexible, and adaptable coordinating structures are essential in aligning the key roles and responsibilities to deliver the Response mission area's core capabilities. The flexibility of such structures helps ensure that communities across the country can organize response efforts to address a variety of risks based on their unique needs, capabilities, demographics, governing structures, and non-

traditional partners."[40] Additionally, "the NRF is not based on a one-size-fits-all organizational construct, but instead acknowledges the concept of tiered response, which emphasizes that response to incidents should be handled at the lowest jurisdictional level capable of handling the mission."[41] This building block approach to response management is an important concept to understand, because without an actual cyber response capability and management process residing at the local incident site level and building up, the NRF's envisioned methods of "tiered response" simply will not work.

The failure of management now follows that from a cyber response perspective, the aforementioned current policy and capabilities envision processes that are managed from the "top down" at both DOD and DHS, versus the "bottom up" structure outlined in the NRF. This approach concerns those looking at cyber response from a state and local perspective. According to Director English, "federal efforts must be structured in concert with states and locals rather than adopting a top-down approach."[42]

Although DHS and DOD processes appear "top-down" focused, the management processes necessary to even address cyber response issues really don't even exist currently. As evidence of these shortfalls, in a recent Congressional hearing titled "*Cyber Incident Response: Bridging the Gap Between Cyber Security and Emergency Management*," Director English stated, "79.1 percent of states interpret the consequences of a cyber-attack under statutes as 'All Hazards' versus 20.9 percent which list it as a specific hazard."[43] Despite cyber incidents now being looked at through an "all hazards" lens, there is no dedicated FEMA Emergency Support Function specifically for cyber to even allow for the procurement and allocation of any cyber response resources. The most current version of FEMA's *Typed Resource Definitions for Incident Management* in 2005 fails to list even a single resource type pre-identified for a cyber

response.[44] What this means is that if a cyber attack hit a municipal energy system today, there is no pre-defined management capability threading from the incident site all the way to the federal level to adjudicate the inevitable resource requests for cyber response and recovery capabilities.

Recommendation

The four failures of imagination, policy, capabilities, and management provide a useful framework for understanding the cyber response capacity gap that exists today. To address this gap, the National Guard, through its on-scene, local presence in every state and territory across the US, is in a unique position to cover-down on these deficits in a credible way ensuring the US develops the necessary resilience to respond and recover from a "cyber 9/11" event.

In testimony to the Senate Armed Services Committee in November of 2011, then NGB Director, General Craig McKinley, stated, "the domestic mission of the National Guard must be taken into account when making military contingency plans, when allocating scarce readiness resources, and when advising the president, the secretary of Defense, the National Security Council and the Homeland Security Council on strategies and contingency response options. Homeland defense and civil support must be at the core of our national strategy due to the changing threat environment, one that is asymmetrical and more dangerous within our homeland than at any time in our history."[45] Given this background setting, the single recommendation of this paper urges both DOD and Congress to take immediate action and establish NG cyber Civil Support Teams (CSTs) to address the cyber response capability gap outlined in preceding sections. The following sections outline a draft framework for addressing the mission, organization, and costs of a notional NG cyber CST force structure.

Mission

As a state response resource, cyber CSTs would be primarily a state domestic response asset, under the day-to-day control of the State Adjutant General. Cyber CSTs would actively build response relationships and partnerships with key CIKR sectors in their respective states and follow existing emergency management frameworks to respond to catastrophic cyber incidents. If an incident escalated, overwhelming state and local assets--including the cyber CST--the governor could request a Presidential declaration, placing the cyber CST in an ideal position to help facilitate any follow-on federal response.

Following the mission format from the existing WMD-CST model,[46] cyber CSTs would be primarily responsible for four main tasks: supporting civil authorities at a domestic cyber incident site through forensic and intrusion analysis; assessing current and projected consequences of the cyber event and resultant second and third order effects from an emergency management perspective; advising on response measures; and assisting with appropriate requests for additional support. Additionally, while in-garrison, cyber CSTs would be given additional missions to work with DHS and partner with CIKR sectors to assess threats and vulnerabilities at existing sites within that particular state or territory. The NG is already performing a mission similar to this through the DHS Vulnerability Assessment Team.[47] However, this team's mission is currently limited to assessing physical threats to critical infrastructure within a given state. The addition of a critical cyber assessment component provided by the cyber CST will strengthen this existing approach, assist DHS in increasing the capacity of CIKR sector cyber assessments, as well as build the trust, credibility, and partnerships with the day-to-day CIKR operators. All necessary processes to ensure a smooth transition from the protection/prevention

phase of the emergency management cycle to actual response and recovery should an event occur.

Organization

Absent from the congressional legislation creating NG cyber CSTs is a proposed organizational framework. Rather than replicating the CPT concept of 39 full-time personnel across all 54 states and territories, as a cyber CST concept, a smaller, less budget-intensive concept should be considered. In evaluating alternative viewpoints for team composition, we should first look to an organization that has extensive experience in managing cyber response issues: Microsoft Corporation. According to Russ McRee, Director of Threat Intelligence for Microsoft Corporation and Cybersecurity advisor for the Washington State Guard, "the premise of a NG cyber CST not only makes perfect sense, but it's the ideal construct for a specialized, rapidly deployable team to respond to significant state-specific cyber security events."[48]

Leveraging his Microsoft experience, Mr. McRee recommends, "a NG team consisting of 14 members who could deploy in four hours or less. At a high level this includes a unit commander, an executive officer or senior NCO, and twelve specialists divided into two squads. Team composition should consist of two-person teams who train and deploy together, including two teams of digital forensics and incident response specialists for attention to direct victim system analysis; two teams of intrusion analysts for activities specific to log and evidence analysis; and two teams of attack and penetration specialists to conduct hunt-like activities during events wherein they would seek out further evidence of compromise."[49] Mr. McRee's recommendations are sound, as this 14 member team represents the skill set balance (outlined in greater detail below) needed in a credible response force, without the possibility of smothering

the attack victim with uniformed military personnel, something the 39-person CPT concept must also consider.

Unlike the WMD-CSTs which consist of 22 full-time members and CPTs with 39 full-time members, the key force multiplier of a cyber CST response force would be found in its mix of full-time vs. part-time members. The cyber CST full and part-time composition mix reflects the need to constantly keep team member technical skills the most current they can be, as skill acquisition and retention simply can't be matched by having all the forces full-time. A recent memorandum titled, *National Guard Cyber Unique Capabilities,* from NGB J-6, only reinforces this point by stating, "many NG personnel possess highly valuable cyber skills acquired through their civilian employment and non-military training. These include, but are not limited to: network auditing, Supervisory Control and Data Acquisition (SCADA), hunting operations, information assurance, and other cyber/IT skills."[50] Hiring part-time members for cyber CSTs from the very corporations they work with on a daily basis is analogous to a "volunteer fire department" and only serves to strengthen the tremendous partnership opportunities between the NG and affected CIKR sectors.

Costs

Using the force mix recommended by Mr. McRee, the cyber CST composition results in four officers (two full time and two part time) and 10 enlisted (two full time and eight part time) members. According to cost planning figures obtained from the ANG for Fiscal Year 2014[51], combined salaries and benefits per team amount to $756,492 or $40,850,568 for 54 teams. Excluding salaries and benefits costs, and focusing on training, equipment, and temporary duty costs results in a per team cost of $154,000 per year or $8,316,000 for 54 teams.

A key hurdle to overcome for any NG response force is to also ensure the proper fiscal authorities exist to allow immediate response. To ensure NG CSTs have the fiscal authority to allow immediate response to cyber incidents, I recommend replicating the budget language existing WMD-CSTs use to fund their operational responses. Specifically, the Fiscal Year 2013 Budget Guidance Document for the Army National Guard includes funds for CSTs in category 121G00 that "funds all costs associated with training, exercises, common and peculiar equipment and equipment repair and sustainment, formulary costs, doctrinal development, training readiness oversight, modeling and simulation tools, general services and support services, operational deployments, and other associated costs for the WMD-CSTs."[52] Important in this language is that this fiscal guidance actually authorizes funds for operational deployments, thereby eliminating the cyber CST's need to request any additional authority prior to employment or deal with DSCA authorities issues.

Conclusion

When our national leaders talk about the possibility of a "cyber 9/11," it is important we first look back and see what lessons we may have learned from our experiences with the actual 9/11 attacks that can now be viewed through a cyber lens. We should look to these lessons and understand how they can apply now to both the cyber threat and our lack of response capacity. What these lessons show us is that we still have failures of imagination, capability, policy, and management; this time not in relation to terrorists using airplanes against buildings, but within our own nation's ability to respond and recover from a catastrophic cyber attack that politicians and senior national leaders concede is a near certainty.

From an imagination perspective, although we realize a catastrophic cyber attack is within the realm of possibility, as a nation, we have done little to create actual response forces that could make a difference where it matters at the domestic state and local level during an attack...the true "ground-zero" for cyber attacks. This is equivalent to saying firefighting is important, but never building a fire department. From a capabilities standpoint, both DOD and DHS acknowledge domestic cyber response is an important capacity; but to date, no dedicated response capability has been created to ensure those at ground-zero of a cyber attack--our state and local authorities--actually have a capability that can be used locally to support on-scene cyber response efforts. Additionally, while DOD continues to develop Title 10 cyber capabilities, none of these capabilities have the primary mission of assisting entities outside of DOD during an attack. From a policy standpoint, both DHS and DOD still struggle with developing clear policy for cyber response and understanding how limited federal capabilities could be made available to state governors. Although cyber response in many ways is just now being contemplated from an emergency management perspective, the speed of resource need and on-scene urgency that would be required in a catastrophic cyber response simply won't hold up to the bureaucracies in place now, such as requesting DSCA authority to even allow a NG federal response for a domestic cyber event. Additionally, from a management perspective, there are clear failures in anticipating cyber resource requirements at the federal level, and viewing cyber response processes from a "bottom-up" versus a "top-down" perspective.

From a NG perspective, these four failures represent yet another opportunity to develop true "paradigm-shifting" domestic Homeland Defense capabilities to protect our citizens from cyber threats in a manner similar to how the NG currently does for other threats such as hurricanes, earthquakes, floods, and WMD events. Worrying about raising a fire department

while the forest is burning is no way to plan. Similarly, exchanging business cards and developing a cyber response capability in the midst of a crippling cyber attack is no way to plan either. We can't simply rely on a pickup team the first time an event happens given the sophistication and scale of the well-documented cyber threats we face. The urgent need for dedicated NG cyber teams located in each state and territory that can quickly respond to a cyber attack, understand private industry concerns, has connections to federal level resources, and understand the interrelationships between the cyber event and the broader emergency management context has never been greater, and must be addressed now.

Notes

[1] Senator Joseph Lieberman, "*Introduction of Cybersecurity Act of 2012*" (floor speech, Washington, DC., 14 February 2012).

[2] The President of the United States, *National Security Strategy, May 2010* (Washington, DC: 2010), 27.

[3] Department of Defense, *Strategy for Homeland Defense and Defense Support to Civil Authorities, February 2013* (Washington, DC: 2013).

[4] United States Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, Report no. GAO-13-187, February 2013 (Washington, DC: 2013), 34.

[5] Ibid.

[6] Cheryl Pellerin, "*Cybercom Builds Teams for Offense, Defense in Cyberspace*," Defense.gov, 12 March 2013, http://www.defense.gov/news/newsarticle.aspx?id=119506

[7] United States Cyber Command J-34, *Cyber Protection Platoons*, 25 March 2013, 21.

[8] *The 9/11 Commission Report*, Washington, DC., 339.

[9] GAO-13-187, 49.

[10] Charley English, *Statement for the Record on behalf of the National Emergency Management Association* (Washington, DC., 30 October 2013), 5.

[11] United States Senate, *Cyber Warrior Act of 2013*, 113th Cong., 1st sess., 22 March 2013.

[12] Patrick Leahy, "*Leahy & Others Introduce Bill To Expand Cyber National Guard*," 22 March 2013, http://www.leahy.senate.gov/press/leahy-and-others-introduce-bill-to-expand-cyber-national-guard

[13] Minutes of the National Guard Cyber General Officer Advisory Council, 13 June 2013, 3.

[14] United States House of Representatives, Subcommittee on Emergency Preparedness, Response, and Communications, "*Joint Subcommittee Hearing: Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management*," (Washington, DC: 30 October 2013), http://homeland.house.gov/hearing/joint-subcommittee-hearing-cyber-incident-response-bridging-gap-between-cybersecurity-and

[15] Govtrack.us, "*S. 658: Cyber Warrior Act of 2013*" and "*H.R. 1640: Cyber Warrior Act of 2013*," https://www.govtrack.us/congress/bills/113/s658 and https://www.govtrack.us/congress/bills/113/hr1640

[16] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: July 2011), 11.

[17] Departments of Defense and Homeland Security, Letter to Governors Terry Branstad and Martin O'Malley, 3 May 2013.

[18] United States Senate, *Senate Report 113-085: Department of Defense Appropriations Bill*, 113th Cong., 1st sess., 1 August 2013.

[19] National Commission on the Structure of the Air Force, *Report to the President and Congress of the United States*, (Washington, DC: 30 January 2013), 40.

[20] Department of Defense, *The Use of the National Guard for Defense Support of Civil Authorities*, Instruction 3025.22, 26 July 2013, 3.

[21] The White House, Office of the Press Secretary, *Presidential Policy Directive -- Critical Infrastructure Security and Resilience: PPD-21* (Washington, DC: 12 February 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[22] Department of Homeland Security, *National Cyber Incident Response Plan: Version 1* (Washington, DC: September 2011).

[23] Ibid, H-1.

[24] Leahy, Patrick.

[25] Department of Homeland Security, *National Preparedness Report* (Washington, DC: 30 March 2013), 24.

[26] Ibid, 8.

[27] The White House, PPD-21.

[28] Department of Defense and the Department of Homeland Security, *Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity* (Washington, DC: 13 October 2010), 1

[29] Department of Homeland Security, *ICS-CERT Year in Review – Industrial Control Systems Computer Emergency Response Team* (Washington, DC: 2012), 14

[30] Bestenergynews.com, *Utility Companies list by State*, http://www.bestenergynews.com/solar/utility_co/utility_companies.php

[31] *ICS-CERT Year in Review*, 14.

[32] Department of Homeland Security, *Dams Sector: Roadmap to Secure Control Systems* (Washington, DC: 2010)

[33] *ICS-CERT Year in Review*, 14.

[34] United States Army Corps of Engineers, *National Inventory of Dams*, available at http://geo.usace.army.mil/pgis/f?p=397:5:0::NO

[35] *Department of Defense Strategy for Operating in Cyberspace*, 8.

[36]Army National Guard, *National Guard CERF-P Teams*, (Washington, DC: 20 December 2010).

[37] Air National Guard, *ANG Cyber Roadmap* (Washington, DC: May 2013).

[38] Minutes of the National Guard Cyber General Officer Advisory Council, 12 June 2013, slide 48.

[39] Department of Homeland Security, *National Response Framework, Second Edition* (Washington, DC: May 2013), 6.

[40] Ibid, 30.

[41] Ibid.

[42] English, Charley, 5.

[43] Ibid, 4.

[44] Federal Emergency Management Agency, *Typed Resource Definitions: Incident Management Resources* (Washington, DC: June 2005), http://www.fema.gov/pdf/emergency/nims/incident_mgmt.pdf

[45] Joint Chiefs of Staff, *Senate Armed Services Committee Testimony on Whether the Chief, National Guard Bureau Should be a Member of the Joint Chiefs of Staff* (Washington, DC: 10 November 2011), http://www.jcs.mil/speech.aspx?id=1658

[46] Washington National Guard, *10th Civil Support Team Capabilities Briefing* (Camp Murray, WA: Feb 2011), 3.

[47] Army National Guard, *Critical Infrastructure Protection Mission Assurance Assessments* (Washington, DC: March 2013), http://www.nationalguard.mil/media/factsheets/2013/CIP-MAA%20-%20March-2013.pdf

[48] Russ McRee (Director, Threat Engineering, Online Services Security & Compliance, Microsoft Corporation), in discussion with the author, 18 November 2013.

[49] Ibid.

[50] National Guard Bureau memorandum, National Guard Cyber Unique Capabilities, NG-J6, 11 April 2013.

[51] National Guard Bureau, *Air Force 2014 President's Budget Composite Rates* (Washington, DC: February 2013).

[52] Army National Guard, *Fiscal Year 2013 Budget Execution Guidance* (Washington, DC: 2013), 88.

Bibliography

Air National Guard, *ANG Cyber Roadmap,* May 2013.

Army National Guard, *Fiscal Year 2013 Budget Execution Guidance*, 2013.

Army National Guard, *Critical Infrastructure Protection Mission Assurance Assessments*, March 2013.

Army National Guard, *National Guard CERF-P Teams,* 20 December 2010.

Army, United States, Corps of Engineers, *National Inventory of Dams.* http://geo.usace.army.mil/pgis/f?p=397:5:0::NO

Bestenergynews.com, *Utility Companies list by State.* http://www.bestenergynews.com/solar/utility_co/utility_companies.php

Carter, Ashton, B. Deputy Secretary, Department of Defense and Lute, Jane Holl, Deputy Secretary, Department of Homeland Security to the Honorable Terry Branstad, Governor, State of Iowa and the Honorable Martin O'Malley, Governor, State of Maryland. Letter, 03 May 2013.

English, Charley, "*Statement for the Record on behalf of the National Emergency Management Association*", Washington, DC., 30 October 2013.

Department of Defense, *Department of Defense Strategy for Operating in Cyberspace,* July 2011.

Department of Defense, *Strategy for Homeland Defense and Defense Support to Civil Authorities,* February 2013.

Department of Defense, *The Use of the National Guard for Defense Support of Civil Authorities*, Instruction 3025.22, 26 July 2013.

Department of Defense and the Department of Homeland Security, *Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity,* 13 October 2010.

Department of Homeland Security, *Dams Sector: Roadmap to Secure Control Systems*, 2010.

Department of Homeland Security, *ICS-CERT Year in Review – Industrial Control Systems Computer Emergency Response Team,* 2012.

Department of Homeland Security, *National Cyber Incident Response Plan: Version 1*, September 2011.

Department of Homeland Security, *National Preparedness Report,* 30 March 2013.

Department of Homeland Security, *National Response Framework, Second Edition,* May 2013.

Federal Emergency Management Agency, *Emergency Support Functions Annexes: Introduction,* January 2008.

Federal Emergency Management Agency, *National Incident Management System (NIMS) Overview,* 2011.

Federal Emergency Management Agency, *Typed Resource Definitions: Incident Management Resources*, June 2005.

Govtrack.us, "*S. 658: Cyber Warrior Act of 2013*" and "*H.R. 1640: Cyber Warrior Act of 2013*". https://www.govtrack.us/congress/bills/113/s658 and https://www.govtrack.us/congress/bills/113/hr1640

Joint Chiefs of Staff, *Senate Armed Services Committee Testimony on Whether the Chief, National Guard Bureau Should be a Member of the Joint Chiefs of Staff,* 10 November 2011.

Leahy, Patrick, "*Leahy & Others Introduce Bill To Expand Cyber National Guard*," 22 March 2013

Lieberman, Joseph, "*Introduction of Cybersecurity Act of 2012*", Washington, D.C., 14 February 2012.

Minutes. National Guard Cyber General Officer Advisory Council, 12 June 2013.

National Commission on the Structure of the Air Force, *Report to the President and Congress of the United States*, 30 January 2013.

National Guard Bureau, *Air Force 2014 President's Budget Composite Rates,* February 2013.

National Guard Bureau memorandum, National Guard Cyber Unique Capabilities, NG-J6, 11 April 2013.

Pellerin, Cheryl, "Cybercom Builds Teams for Offense, Defense in Cyberspace," Defense.gov, 12 March 2013. http://www.defense.gov/news/newsarticle.aspx?id=119506

President. *National Security Strategy*, May 2010.

US Cyber Command. Cyber Protection Platoons, J-34. 25 March 2013.

US Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, Report no. GAO-13-187, February 2013.

US House, Subcommittee on Emergency Preparedness, Response, and Communications, "*Joint Subcommittee Hearing: Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management*," (Washington, DC: 30 October 2013).

US Senate, *Cyber Warrior Act of 2013*, 113th Cong., 1st sess., 22 March 2013.

US Senate, *Senate Report 113-085: Department of Defense Appropriations Bill*, 113th Cong., 1st sess., 1 August 2013.

Washington National Guard, 10th Civil Support Team Capabilities Briefing, Feb 2011.

White House, Office of the Press Secretary, *Presidential Policy Directive -- Critical Infrastructure Security and Resilience: PPD-21*, 12 February 2013.